Kuo, P-H., Mourad, A. y Ahn, J. (2018). Potential Applicability of Distributed Ledger to Wireless Networking Technologies. *IEEE Wireless Communications*, 25 (4), pp. 4-6.

DOI: 10.1109/MWC.2018.8454517

Potential Applicability of Distributed Ledger to Wireless Networking Technologies

Ping-Heng Kuo and Alain Mourad, InterDigital Europe Ltd, London, United Kingdom
Jaehyun Ahn, InterDigital Asia Ltd, Seoul, Korea

Introduction

In recent years, the rise of cryptocurrency (e.g., Bitcoin [1]) has received enormous attention around the world. Since a centralized entity (e.g., a bank) is no longer needed for transactions in this currency platform, its potential impact on the financial sector in the future has been examined closely. Apart from the transaction platform itself, the driving technology behind cryptocurrency, namely blockchain, has also kindled huge research interest across different disciplines. A report [2] published recently by the European Commission (EC) discussed how blockchain could be applied to transform various types of industries in the future, including food processing, transportation, health, energy, and so on. In fact, blockchain (and its variants) can be deemed as a branch of a broader technology family dubbed distributed ledger technologies (DLTs). Generally speaking, a distributed ledger is essentially a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, without needing a central administrator or centralized data storage as in previous technologies.

Notably, DLTs can be employed to facilitate maintaining a common view (or more precisely, a consensus) among a group of geographically distributed but inter-connected nodes without a central controller. Such a consensus could be referred to as an archive of transaction record, a policy/strategy to be applied jointly by several parties, or a configuration of multiple machines. It is straightforward to see that the dispersed scenario targeted by DLT matches numerous use cases in existing and future wireless networks. For instance, such a distributed topology can be seen in an ad hoc network comprising mobile devices running without a base station or an access point, or a dense cluster of small cells serving a hotspot area. More examples of distributed networks can be anticipated in fifth generation (5G) and beyond, due to new use cases involving collaborations among devices. Hence, it is indeed worth pondering how DLT could be applied to facilitate or enhance wireless networking technologies in different aspects.

The rest of this column begins with a glimpse at the concepts of some more commonly known DLTs, including both blockchain and hashgraph [3]. Then we highlight the fact that research activities on DLT applications to network security are already gaining some momentum. Finally, we describe how DLT can potentially be further employed to streamline wireless networks beyond security, especially from the perspectives of radio access connectivity and computing.

Review of DLT

DLT can be applied to a group of nodes to facilitate achieving a common database among the nodes that are geographically distributed. All the entries of this database are duplicated at every member node, so they can share a global view despite their distinct locations. In comparison to former database technologies, DLT does not require the intervention of a centralized controller. Such a characteristic makes malicious attacks such as data tampering very difficult because it means the attacker can only alter the database contents based on the validation of numerous other nodes. Moreover, the database is more robust against malfunction or unavailability of the machines due to diversity provided by data duplication.

The key component of DLT is the consensus mechanism — that is, how the consensus should be made and maintained among multiple parties. In order to enter new entries to a distributed ledger, a member should propagate such a request to its peers, who will then attempt to validate such a transaction prior to announcing its legitimacy and adding it to the accumulating ledger. Once a member has validated a transaction successfully, it should announce the result so that other members can add this new entry as well. Similarly, invalid transactions will be discarded. It is notable that each member carries out the validation and insertion of a transaction by itself without any centralized mediator. This is because a consensus rule is pre-defined, and all members are aware of this. Thus, the database is updated among the members with synchronicity. For example, the DLT platforms used by some more well-known cryptocurrencies such as Bitcoin and Ethereum have adopted a proof-of-work (PoW) [4] concept for transaction validation in the group. The PoW, also known as mining, requires each member to find an appropriate hash value that satisfies the pre-defined condition in accordance with the consensus rule before broadcasting a block of transactions they wish to add, and the members that receive such a block will simultaneously begin to attempt validating such a block.

The PoW is beneficial in terms of strong security against attack by malicious users due to the high demand of computing power. Nevertheless, it has the shortcoming of long latency due to the time needed to validate transactions. Therefore, its applicability to delay-sensitive use cases such as lower-layer protocol stacks of a communication system are more questionable, and further research is required. Correspondingly, several other forms of DLT with simplified PoW procedures have emerged. For instance, Hyperledger [5] uses the practical Byzantine fault tolerance (PBFT) method, in which a block is distributed and, if at least two third of members confirm the block, it is committed as part of the blockchain. Parity [6] implements a simplied version of proof of stake (PoS). PoS selects a node that can append a block by its investment (or stake) in the system, which should be a trusted node. On the other hand, as a departure from PoW-based mechanisms discussed above, a DLT such as hashgraph [3] features a consensus mechanism that is based on a virtual voting algorithm on top of a gossip communication protocol, which allows the member devices to reach consensus more efficiently with lower power consumption.

DLT for the Internet of Things

As aforementioned, the most prominent feature of DLT is its capability of information tracking, updating, and coordinating information among multiple independent distributed nodes, without needing a centralized entity. In view of networking technologies, this feature becomes appealing when the number of connected devices within a network grows, as management of a large number of distributed devices may become increasingly cumbersome in practice.

Against this backdrop, many research initiatives have been conducted in recent years to study how DLT could be used

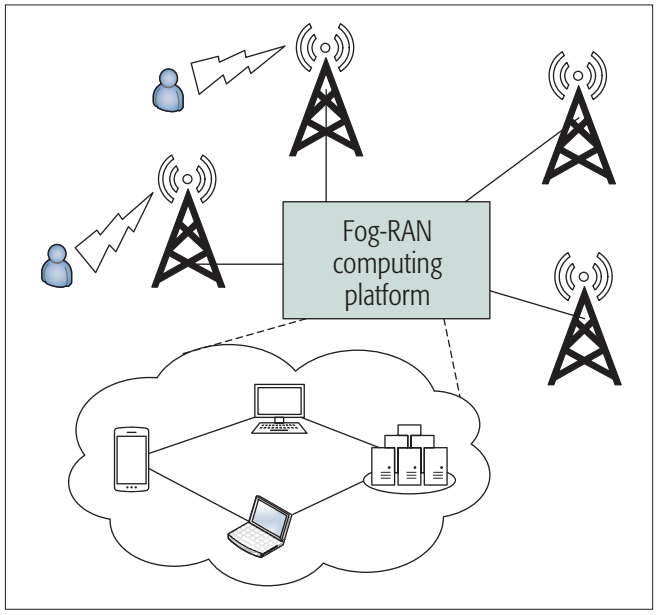

FIGURE 1. An illustration of RAN assisted by Fog Computing, wherein the computing platform is composed of distributed devices.

in the Internet of Things (IoT) [7], which envisages inter-connections among a massive number of devices ranging from low-cost sensors/actuators to high-end cameras. Obviously, IoT is promising in terms of realizing visions such as smart city and Industry 4.0. Nevertheless, handling security and privacy for numerous connected devices as anticipated in IoT can be quite challenging. Specifically, with the classical security architecture, a central authority (e.g., a cloud data center or a server farm) is employed as a single-point security intelligence that manages and aggregates all trust requests coming from the devices. Therefore, the security of an IoT network could be breached due to a single point of failure. It makes the network vulnerable to attacks such as denial of service (DoS), in which the attackers may easily stall the central server by flooding it with traffic using compromised devices. Additionally, there are also concerns on how the centralized architecture can be scaled and managed in a cost-effective manner as the number of connected devices continues to grow.

Instead of relying on the centralized architecture that is vulnerable to a single point of failure and difficult to scale, a decentralized security approach may be more desirable for IoT use cases with massive connections. From this point of view, DLT has great potential in offering viable solutions to address security challenges of IoT. In particular, a secure mesh network can be created via DLT, wherein every registered device can identify and authenticate each other without needing the central entity. Thus, a transaction between two untrusted devices can still proceed securely even if the central entity is absent, as validity of such a transaction can only be confirmed based on consensus among all peers. More details about how DLT (particularly blockchain) can be applied to IoT can be found in [8].

As elaborated, nowadays the scope of DLT in telecommunications has been largely focused on security and privacy issues. However, we foresee DLT playing a more extensive role in future wireless networking beyond the application and security layers. It is apparent that we are seeing more radio access network (RAN) topologies migrating to a more decentralized nature, considering the emergence of self-driving devices (e.g., drones, autonomous cars, and robots) and direct connectivity technologies (e.g. device-to-device and vehicle-to-vehicle), as well as new use cases that require close coordination among these devices (e.g., a platoon of cars, or tasks to be executed by a group of robots).

Paradigms of Consensus-Based Connectivity and Computing

Following the argument made previously about the trend of decentralization in the network, in this section we present examples of how the consensus among multiple nodes can facilitate connectivity and computing in a communication network. More specifically, we see DLTs as potential enabling mechanisms for more efficient fog-RAN operations and grant-free access schemes, as discussed below.

Fog-RAN

Autonomy is indeed the most noticeable difference between these new terminals and the traditional handsets, as potentially they are capable of manoeuvring and making certain decisions themselves without human intervention. This characteristic may allow them to assist the network in terms of extending radio coverage and/or expanding computing power, which leads to a network with an architecture comprising dynamic placement of nodes. Remarkably, the exploitation of computing resources of these devices leads to the paradigm envisioned by fog-RAN, in which computing tasks pertaining to a RAN can be partitioned and executed across multiple nodes, including devices on the move (as depicted in Fig. 1). It essentially stitches distributed nodes at the network edge into a logical computer, as the resources (for computing, networking, and storage) available in different devices and locations can be jointly leveraged for execution of certain network functionalities or application tasks. Such a framework enables various types of new wireless services, including intelligent transportation systems, haptics/tactile Internet, and virtual reality (VR). Due to the stringent latency and reliability requirements of some of these applications, intelligence needs to be enabled all along the continuum from the cloud to the end-user terminal where data is generated. The feasibility and applicability of fog-RAN are currently being studied by several research projects and consortia including 5G-CORAL [9].

The tight synchronization among the geographically dispersed devices is obviously needed to enable collaborative mechanisms. Thus, it is envisaged that DLT could be employed to reach different levels of consensus among distributed nodes (including both mobile terminals and infrastructure entities) that are required for them to conduct a multitude of collaborative operations. Additionally, as time goes by, the ample data maintained in the distributed ledger can be useful for effective data-demanding algorithms such as deep learning.

Grant-Free Access

Uplink transmission in cellular systems such as Long Term Evolution (LTE) is typically based on a scheduling request and grant-based access mechanism. That is, a user terminal will have to first request a radio resource and then receive a grant from the base station before carrying out uplink transmission. However, for cases such as machine type communications, this scheduling and grant-based procedure is not so suitable as the ratio of the resultant signaling overhead might be of the same order as the payload itself, especially because the packet sizes of sensor readings are typically very short. To address this issue, the concept of grant-free uplink transmission has been proposed. With grant-free uplink access [10], once the devices have data in the buffer, they can instantly transmit on pre-configured or randomly selected radio resources instead of waiting for grants. However, when more than one device attempt to carry out

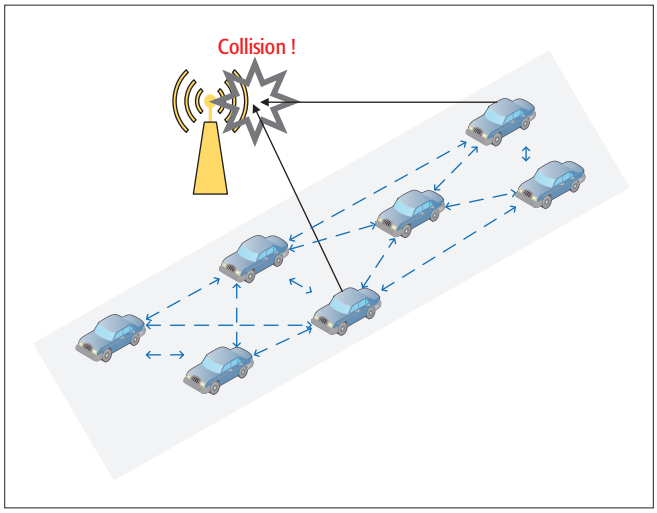

FIGURE 2. Resource collision problem for grant-free uplink access. DLT could be applied to solve this issue based on consensus of resource usage among devices.

uplink transmission simultaneously, the base station may not be able to resolve the signals from multiple devices into the same radio resource. Figure 2 shows such collision when two vehicles in a car platoon conduct uplink transmission concurrently. Therefore, although complicated signaling between the base station and each car/sensor could be avoided with grant-free uplink access, it also causes inevitable resource collisions that will eventually degrade the system performance.

With assistance of DLT, the devices within the group may first reach a consensus about what radio resources each member of a device group should use when they have data to transmit in uplink. The detailed consensus-making procedure depends on which DLT is being applied, but basically each device may propose a subset of resources (e.g., a set of subframes and/or a set of subcarriers) it intends to use for grant-free uplink, and such a proposal will be validated and agreed on by its peers prior to adding to a common database. Eventually, the database of resource usage is duplicated at every device thanks to the DLT property, and a consensus is thereby reached. Hence, each device is aware of the resources it should be using, as well as the resources that have been reserved by other members. This results in a grant-free uplink scheme without collision due to consensus made in advance.

Conclusions and Beyond-5G Visions

The decentralized nature of existing and future wireless network topologies has opened some unique opportunities for DLT to play a role in communications. In this column, we have reviewed the basic operation of a consensus mechanism, as well as the current trend of a DLT-based security model that is particularly important for IoT. We further point out that, beyond application layer and security, DLT also has potential in other aspects of wireless networking such as computing and radio connectivity. Specifically, we see DLT as a perfect tool that should be leveraged to realize fog-RAN, as the consensus mechanism of DLT may be used to maintain tight synchronization among computing and networking resources in different locations. On the other hand, DLT could also be employed to avoid potential collision that may occur in grant-free uplink access. In summary, we believe that DLT will gradually become a key tool to reshape communication systems in a wide range of aspects, covering not just applications and security, but also connectivity and computing.

Acknowledgment

This work has been partially funded by the H2020 collaborative Europe/Taiwan research project 5G-CORAL (grant no. 761586).

References

[1] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly, 2014.
[2] "Blockchain4EU: Blockchain for Industrial Transformations," Joint Research Centre, EC, 2018.
[3] L. Baird, "The SWIRLDS Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance," SWIRLDS-TR-2016-01, May 2016.
[4] https://en.bitcoin.it/wiki/Proof_of_work
[5] https://www.hyperledger.org/
[6] https://www.parity.io/
[7] Y. Gupta *et al.*, "The Applicability of Blockchain in the Internet of Things," *Proc. 10th Int'l. Conf. Commun. Systems & Networks*, Jan. 2018.
[8] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, May 2018.
[9] http://5g-coral.eu/
[10] A. Azari *et al.*, "Grant-Free Radio Access for Short-Packet Communications over 5G Networks," arXiv: 1709.02179v1 [IT], Sept. 2017.